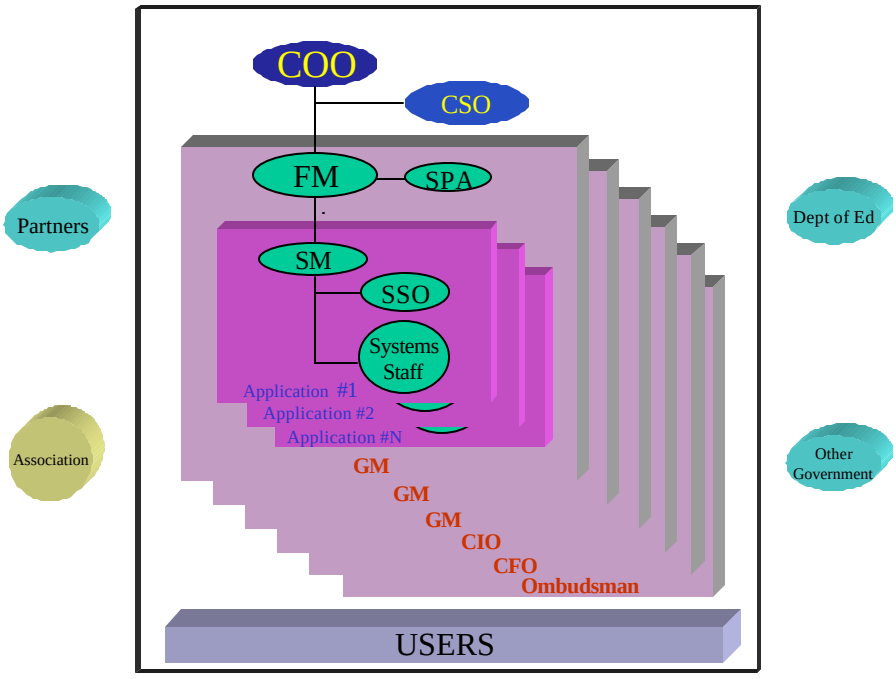
The SFA Security Organization

The security management team in SFA is composed of approximately 25 members who are accountable for implementation and administration of SFA security. The security management structure is aligned with the business management structure of SFA. An SFA business manager usually wears a second hat as an SFA security manager. The notional organizational chart below depicts the SFA Security & Privacy structure surrounded by the outside entities which also play roles in SFA Security & Privacy.



The following pages describe each SFA security manager's roles and responsibilities; "users" don't have a managerial role, so they are only included within this document as a part of the chart.

The ***Chief Operating Officer*** (COO) is responsible for operation of all SFA systems. The COO appoints functional managers, who manage the business operations of SFA, and he appoints the Computer Security Officer, who is responsible for policy, guidance, and development of the SFA security architecture. Ultimately, responsibility for security falls to the COO as the head of SFA.

- **Maintain** overall responsibility for securing SFA data and information systems
- **Maintain** overall responsibility for the establishment and review of SFA security and privacy policy
- **Appoint** a Computer Security Officer (CSO) as the SFA security advocate
- **Create** the Information Security and Privacy Working Group and implement recommendations as necessary

- **Encourage** Department of Education and extra-Departmental (GAO, OMB, etc.) participation in SFA security and privacy matters

The ***Computer Security Officer*** (CSO) and his staff are dedicated to security and privacy within SFA. The CSO is the Security & Privacy Champion. Appointed by the COO, the CSO implements and maintains the SFA IT security program. He advises the SFA Management Council and works closely with Department of Education security officials. He coordinates security policy and directives and supports the Security & Privacy Advocates (SPAs) and System Security Officers (SSOs) associated with the Functional Managers (FMs).

- **Review** Department of Education and government wide policy and incorporate it into SFA policy
- **Issue** designation letters identifying FMs, Data Owners, Designated Accreditation Authorities (DAAs), SPAs, and Certifying Officials (COs)
- **Appoint** primary points of contact for security incidents of all types
- **Receive** and **act** on notifications of security and privacy incidents
- **Meet** regularly with Department and SFA security officials
- **Maintain** overall responsibility for the SFA Security & Privacy website
- **Head** periodic or ad hoc security working groups
- **Coordinate** responses to external requests for security information about SFA
- **Coordinate** A-130 reviews and penetration tests with security managers
- **Document** and maintain security standards for new hardware or information systems which operate on Departmental networks
- **Maintain** records of and **review** the System Security, Disaster Recovery, Contingency and Continuity of Operations Plans for each information technology installation and system within SFA
- **Make sure** physical security requirements are met for each SFA information technology installation and system
- **Establish** and **enforce** policies on introduction and removal of hardware/software into and from SFA systems and facilities
- **Review** all contracts for compliance with SFA security policy and assist the FM and the Contracting Officer with these efforts
- **Help develop** standard language and / or performance standards on security and privacy for SFA contracts

The CSO is supported by a staff of three to four people who oversee key elements of the SFA Security & Privacy Program. They are the contact points for SFA security managers or users with questions or concerns about policy, compliance, or training.

- As a member of CSO staff, the *Policy Officer*'s job is to make sure all relevant external security policies, guides, mandates and legislation are incorporated into SFA policies as needed. As SFA creates a new policy or a policy change occurs, the Policy Officer updates SFA policy documents and informs the appropriate security managers. The Policy Officer is predominantly involved in the areas of SFA system and business operations. He interjects himself into the SFA procurement system, making sure the SMs and COTRs apply security policies as they purchase software, hardware and services. This policy function may be reserved for one staff member or included with the functions of another staff member, for example the Compliance

Officer. In any case, the CSO staff works as a team with the SPAs to develop and implement security policy in SFA.

- The *Compliance Officer* makes sure SFA security managers implement SFA security policy. He works mainly with the SSOs and SPAs to make sure all users follow policy. He plays a part in incident handling by generating enterprise-wide security reports and updating the SFA-wide Incident Handling Plan as needed. The CSO can also appoint him as the primary point of contact for security incidents that span multiple applications and managers.

  Outside of incident response, the Compliance Officer makes sure all SFA systems have up-to-date Disaster Recovery, Contingency, Continuity of Operations, Configuration Management, Configuration Change, Certification, and Risk Assessment plans. The Compliance Officer works with the SPAs and SSOs to make sure the plans are followed, including such steps as spot checks or inspections to see how well policy is followed. To conduct such compliance sampling, the Compliance Officer works with SSOs and SPAs to maintain useful checklists. The compliance process is applied to existing SFA systems and SFA systems under procurement.

- The *Training Officer* works closely with SFA University and with Department of Education training officials and the SPAs to make sure new SFA employees receive security training within 30 days of arrival and all employees receive annual refresher training. He maintains and develops training materials and assists in training SFA employees as needed. He reviews commercial-off-the-shelf (COTS) security and privacy training packages and identifies outside training opportunities. He organizes periodic security workshops with the help of the CSO staff and the appropriate security managers. He helps the SMs as needed with any system security training or education issues that arise.

- A *Communications Officer* supports the CSO staff, keeping abreast of security and privacy news and maintaining or coordinating maintenance of the SFA Security & Privacy website. He makes sure security information gets out to the appropriate security managers or all SFA users. He distributes information using the SFA Security & Privacy website, email, voice mail or any other appropriate method. He makes sure the website and periodic progress reports accurately indicate systems status and incidents, and that all other website components are current. The Communications Officer is the CSO staff member who reviews security-oriented websites and trade journals to pass relevant news on to SFA security managers.

The ***Functional Managers*** (FMs) in SFA are the main-line business managers who have one or more SFA IT systems under their control. Currently, the FMs are the three General Managers (for Students, Schools and Financial Partners), the Ombudsman, the Chief Information Officer (CIO) and the Chief Financial Officer (CFO). (The CIO is responsible for *infrastructure* systems, such as data center, telecommunications networks, and data warehouses.) The FMs make business decisions about the systems they operate – including making security investments, certifying systems as ready to operate, and

agreeing to operate with identified residual levels of systems risk. FMs are responsible for establishing, maintaining, and enforcing security and privacy of the IT systems under their control. FMs are also Data Owners and Accrediting Officials for their systems. FMs appoint System Managers (SMs), System Security Officers (SSOs), and Security and Privacy Advocates (SPAs).

- **Designate** a SSO for each information system
- **Appoint** a SPA to advise on security and privacy matters
- **Hold** SSOs, SMs and SPAs accountable for assigned security duties
- In role as the DAA, **accredit**, no less frequently than every three years, each assigned system as authorized to operate
- In role as Data Owner, **establish** data elements designated as sensitive information
- **Review** future development efforts with the CSO, SPA, SM, and SSO to make sure that security is handled in a consistent manner across SFA, and that it complies with Departmental and government wide security and privacy requirements

Each FM appoints one or more ***Security and Privacy Advocates*** (SPAs) to serve as staff-level advisors on all security and privacy matters. A SPA is not directly involved in managing IT systems and so embodies the "separation of duties" doctrine. The SPA reports to the FM for purposes of the SFA security and privacy program. SPAs consult with the CSO, SMs, SSOs and others to provide the best possible counsel to the FM. SPAs stay current on security and privacy related events and training, and help disseminate policy originating from the CSO. A SPA may also perform non-security functions in SFA as long as those functions are distinct from the IT systems he supports in his role as SPA.

- **Provide advice** and **counsel** to the FM, SSOs and System Managers in all security and privacy matters
- **Review** current events, training notices, and impacting policy and help disseminate within the organization
- **Coordinate** closely with the CSO to identify issues, define solutions, and monitor progress
- **Participate** in SFA-sponsored security and privacy working groups
- **Make sure** staff get required security and privacy training

Every SFA IT system is managed by a ***System Manager*** (SM), appointed by the relevant FM. IT security is only one component of the SM's job. The SM is responsible for all aspects of the system, including managing risk and ensuring security and privacy. The SM may or may not be the Contracting Officer's Technical Representative (COTR) for contracted systems. The SM serves as the Certifying Official for the system under his/her control.

- **Make sure** detailed position descriptions exist that define role-based system privileges
- **Create** a system-specific list of approved software
- **Create** procedures for users to request SFA-approved software
- **Establish** processes to protect the integrity of the information contained in the materials and data passed from one person or system to another
- **Identify** system information exchanges and comply with the exchange standards
- **Establish** specific training requirements for users and managers of the system

- **Designate** control areas for areas supporting the system
- **Make sure** all system development efforts are accomplished exclusively in a development environment that reflects the operational environment, and tested with approved test data to reduce the risk of compromising data
- **Review** system risk assessment and risk mitigation strategy at least every three years
- As designated Certifying Official, **certify / re-certify** that system meets applicable SFA and Federal policies, regulations and standards
- **Forward** system certification and accreditation package to DAA (FM), brief FM and SPA on certification findings and recommend accreditation outcome
- **Review** expected system event procedures, such as system start-up and initialization, system shut-down, database updates, and software changes
- **Act** on reported security and privacy incidents by approving remedies and notifying FM and CSO
- **Make sure** configuration and change management policies are followed when making system or system environment changes
- **Make sure** requests for proposals include security and privacy requirements
- **Make sure** contractors analyze the operational and security impacts of proposed system changes
- **Make sure** contractors develop a security plan for the system and the plan is updated annually
- **Make sure** contractors develop a System Security Plan, Disaster Recovery Plan, Contingency Plan, and Continuity of Operations Plan for the system

Every SFA IT system also has a ***System Security Officer*** (SSO), appointed by the relevant FM. The SSO is part of the SFA management team overseeing development and operation of the system, but deals solely with the security and privacy issues of the assigned system. The SSO works closely with any contractor security personnel, the CSO, the SPA(s) and other SSOs to make sure all necessary steps are taken to ensure security and privacy in development, testing, and operation of the system. The SSO is the primary point of contact for the personnel clearance process for SFA employees and other personnel who participate in development and operation of the system. The SSO advises the SM in certifying the system.

- **Coordinate** with SM to determine appropriate security requirements for system
- **Develop** and **implement** access lists to controlled areas and information systems for individual users based on role
- **Make sure** necessary physical security is in place to protect system assets
- **Advise** SM on identifying controlled areas
- **Authorize** movement of equipment into or out of controlled areas
- **Develop** escort procedures to allow non-cleared individuals access to controlled areas
- **Coordinate** requests for access with personnel clearance office
- **Develop** media marking, physical control, storage and disposal requirements for assigned sensitive information
- **Make sure** audit tools are used to track user activities on the system
- **Identify** and **limit** access to networks, applications, utilities and scripts based upon role
- **Make sure** procedures for issuing and managing passwords are followed
- **Create** and **maintain** a process that makes sure user lists are kept current
- **Advise** and **consent** on contractor recommendations for system procedures and changes that affect system security and / or privacy

- **Review** and **recommend** changes to the security aspects of the system's Disaster Recovery Plan, Contingency Plan, Continuity of Operations Plan and System Security Plan
- **Conduct** a system risk assessment at least every three years and develop a risk mitigation strategy
- **Control** access to remote / dial-up facilities and **protect** these facilities from unauthorized use
- **Determine** the need for encryption technologies where sensitive data transmissions occur
- **Make sure** the necessary security controls exist to operate the LAN / WAN
- **Consider** disaster recovery procedures prior to physical routing of network cable and the physical location of network support equipment
- **Develop** and **monitor** security controls for assigned system and report control status to SM
- **Monitor** security events of the system and report anomalies to SM and CSO
- **Support** the FM in identifying and developing security requirements for new systems and system enhancements
- **Document** expected system event procedures, such as system start-up and initialization, system shut-down, database updates, and software changes
- **Document** abnormal events, such as system failures, unsuccessful system initializations or shut-downs, system error responses, and corruption or loss of data